

Reporting Data Loss: Tough Choices, One Answer

June 2010



ON CYBER PATROL



As covered or mandat

When a military data is lost, stolen or compromised, the potential dangers are obvious. Lost personal data can lead to identity theft, lost operational data can lead to mission cancellation or failure and lost technical data can lead to other compromised systems and even further damage. While loss of data is bad enough, sometimes the loss is not mitigated in a timely fashion. When this happens, it is often not because of a stealthy hacker or a missing hardware audit. It is because somebody did not report the incident out a fear of potential personal consequences. We need to change that mindset. Not accepting responsibility and warning others of a network or data breach can put missions and lives at risk.

So if you are the cause or you discover a loss of data or a hacked network, it's decision time. Report it or cover it up. What's worse? A chewing out from your CO or knowing that letting your error go unreported resulted in an ambush or the identities of fellow soldiers and their families being stolen? Even if the person that discovers the loss is not personally responsible for the incident, they might be reluctant to report it because it would reflect badly on friends or the unit.

Military personnel tend to have the "not on my watch" mindset. This is a great attribute when it comes to the defense of a position or ensuring that everyone makes it back from a patrol. However, when such dedication to that statement means that fellow soldiers are at risk because of an unreported breach of network security, it is unacceptable. Neither is taking a "not my problem" attitude. Loss or compromise of military data is everyone's problem.

Most soldiers will take responsibility if they are at fault. But many of these same soldiers will cover for a buddy's mistake. Covering for someone is often considered being a team player. That's fine, if you help Bill get ready for inspection after a tough night of leave or taking on more work because Ed needs to deal with a family matter. However, covering for someone in the case of data loss is as risky as not reporting your own error.

Fear is often the motivation for not reporting an incident. Nobody wants to get chewed out or written up. But think about what could happen if data has been compromised and nobody that can do something to eliminate or reduce the problem is ever told. The punishment for not reporting a network security problem that is found out later will be much greater than reporting it in the first place. It's like when you were a kid. Do you tell your parents? It's basically the choice between a scolding and being grounded for a month. In the military, grounding can take the form of docking your pay or sending you to someplace you really don't want to be. But the real issue is not a personal one. The fact is that delay in reporting lost or stolen data can result in lost identities, compromised missions and possibly risk to soldiers in theater.

If you discover a network security breach you should report it to the proper authorities immediately. That's a regulation. Take what steps you can to discover the details of the breach and make those known as well. Do not be influenced by anyone trying to prevent you from taking those steps. It will still be you on the line. Nobody's hard feelings are worth a black mark on your service record. If anyone thinks this is kissing up or not being a team player, imagine what you would think if you were caught in an ambush or had your personal data stolen because someone didn't report a data loss.

In the end, discovering an information loss incident gives you three options. Cover yourself, cover for someone else or be a soldier and take responsibility. "Be a soldier and take responsibility" is the only one right answer!